

La formulazione dell'accusa e le attività d'indagine in tema di criminalità tecnologica

Università degli Studi di Milano

Dipartimento di Informatica e Comunicazione

Dr. G. Braghò, Dr. F. Cajani

COMPUTER FORENSICS, INVESTIGAZIONE PENALE E CRIMINALITÀ
TECNOLOGICA - L.E.F.T. (Legal Electronic Forensics Team)

<http://www.avanzata.it/left> - Milano, 21 dicembre 2006

Sintesi dell'intervento

A cura del Magg. CC Ing. Marco Mattiucci - Roma, 2 gennaio 2007

I pubblici ministeri relatori hanno presentato innanzitutto ed in linea generale la struttura della Procura di Milano, facendo specifico riferimento al 7° Dipartimento che si occupa, tra i diversi settori di competenza, anche di quello informatico.

Si è quindi passato a considerare le varie tipologie di reati connessi all'aspetto informatico classificando, come noto, le seguenti aree:

- a) Crimini informatici in senso stretto;
- b) Violazioni della legge sulla privacy;
- c) Violazioni del diritto d'autore;
- d) Frodi tramite carte di credito su circuiti informatici/telematici.

Molto interessante è stata la dettagliata analisi dei numeri relativi a queste diverse classi di reati (2004-2006) che sono passati per la Procura di Milano. Preponderante, in senso assoluto, la quantità di frodi informatiche (art. 240-ter. CP). Problematica la situazione in relazione al considerare o

meno un reato in ambito informatico. I sopra citati numeri sono infatti alterati dal fatto che spesso, reati che riguardano fattispecie non informatiche, vengono associati a tale ambito solo perché avvengono mediante uno strumento digitale o più comunemente telematico. L'esempio classico è nella frode su EBay che può manifestarsi in un prodotto difforme da quello desiderato. Si tratterebbe ovviamente di una frode classica e non un reato informatico. Il fatto che EBay operi in un ambito telematico non vuole dire che le frodi su EBay sia reati informatici. Tale concetto è talvolta di difficile comprensione per i non addetti per cui si generano confusioni.

La discussione è poi continuata trattando del concetto di scena del crimine reale contrapposto a quello di scena del crimine virtuale. È stato riportato un caso emblematico di reato grave susseguito all'acquisto fraudolento di un oggetto virtuale su Internet (oggetto in un gioco di ruolo telematico). Si è evidenziato come nelle scene del crimine reali l'acquisizione di determinate fonti di prova viene raramente messo in discussione dalle parti mentre in quelle virtuali si tende a discuterle con sempre maggiore enfasi, anche nel caso che le probabilità che le fonti digitali vengano alterate siano estremamente basse. Questo basandosi sulla difficoltà di inquadrare univocamente la virtualità sia in ambito tecnico che legale.

Si è ribadito quindi che *“la miglior pratica forense è quella che non reca danno all'elemento di prova e lo presenta bene in dibattimento”* e che l'acquisizione delle fonti di prova, per quanto particolari è regolata in Italia unicamente dal codice di procedura penale non da particolari manuali tecnici (che semmai è onere e responsabilità diretta del consulente, perito o PG incaricati di attenersi durante le operazioni).

In questo delicato settore del reperimento delle fonti di prova si è quindi parlato delle problematiche legali legate alla identificazione delle informazioni strettamente correlate al procedimento per cui si opera, alla forma dei decreti di acquisizione, in particolare della leggerezza con la quale l'indirizzo IP viene spesso impiegato come identificatore quando è ben noto che raramente oggi porta ad un preciso apparecchio telefonico (tramite ISP e CLI) e quindi ad un edificio quanto piuttosto a reti LAN, WLAN o cellulari. Si è sottolineato come l'anonimato legato al IP è enorme anche perché tecnicamente parlando l'IP non è nato per identificare soggetti ma nodi su Internet, anche se temporanei.

Altri problemi trattati sono stati:

- Individuazione dell'hardware da sequestrare;
- Individuazione dei dati da sequestrare;
- Validità e ripetibilità della copia sul posto;
- L'agente provocatore nelle indagini sul P2P.

Un argomento che ha trascinato relatori e uditori ad una accesa ed interessante discussione è stato infine quello della differenza tra intercettazioni telefoniche e telematiche.

L'art. 266 cpp¹ riguarda le intercettazioni telefoniche mentre il 266-bis² I comunicazioni informatiche o telematiche. Il secondo notoriamente ha meno restrizioni nel suo impiego al primo e la ragione di questa scelta del legislatore è di favorire le attività di indagine su Internet. A questo punto sorge l'inevitabile perplessità: *“ma una chiamata VoIP che viaggia su Internet può o deve essere intercettata secondo il 266 o il 266-bis?”*. La risposta è ovviamente che deve essere intercettata ai sensi del 266-bis in quanto flusso digitale telematico, ma da questo segue che l'intercettazione telefonica su VoIP ha meno restrizioni di una su canale telefonico standard. A questa affermazione alcuni elementi del pubblico hanno evidenziato la difficoltà di individuare canali telefonici “standard” basata sul fatto che la maggioranza di tali comunicazioni viaggia ormai proprio su canali VoIP per l'indiscutibile risparmio economico che determina, ciò anche a insaputa dell'utente. In definitiva il 266 rimarrebbe confinato alle *“intercettazioni di comunicazioni tra presenti”* ed altra importante conseguenza potrebbe essere che *“vi sia un implicito possibile abbassamento delle garanzie per l'utente”*. È stato fatto notare per finire come lo slittamento verso il 266-bis sia inevitabile anche in relazione agli SMS, MMS, ed altre forme di messaggistica telematica che i cellulari tendono sempre più a supportare.

Si fa riserva di integrare il presente testo con altri dati ad oggi non disponibili...

¹ Art.266 CPP Limiti di ammissibilità

1. L'intercettazione di conversazioni o comunicazioni telefoniche e di altre forme di telecomunicazione è consentita (226 coord.) nei procedimenti relativi ai seguenti reati:

a) delitti non colposi per i quali è prevista la pena dell'ergastolo o della reclusione superiore nel massimo a cinque anni determinata a norma dell'art. 4;

b) delitti contro la pubblica amministrazione per i quali è prevista la pena della reclusione non inferiore nel massimo a cinque anni determinata a norma dell'art. 4;

c) delitti concernenti sostanze stupefacenti o psicotrope;

d) delitti concernenti le armi e le sostanze esplosive;

e) delitti di contrabbando;

f) reati di ingiuria, minaccia, molestia o disturbo alle persone col mezzo del telefono.

2. Negli stessi casi è consentita l'intercettazione di comunicazioni tra presenti. Tuttavia, qualora queste avvengano nei luoghi indicati dall'art. 614 c.p., l'intercettazione è consentita solo se vi è fondato motivo di ritenere che ivi si stia svolgendo l'attività criminosa.

² Art. 266-bis CPP Intercettazioni di comunicazioni informatiche o telematiche

1. Nei procedimenti relativi ai reati indicati nell'art. 266, nonché a quelli commessi mediante l'impiego di tecnologie informatiche o telematiche, è consentita l'intercettazione del flusso di comunicazioni relativo a sistemi informatici o telematici ovvero intercorrente tra più sistemi.